دراسات، علوم الشريعة والقانون، المجلّد 46، عدد 4، 2019

الإثبات الجزائي في جرائم الإرهاب الالكتروني وفقاً للقانون الأردني

مالك نادي سالم صبارنة *

ملخص

الإثبات هو إقامة الدليل أمام القضاء بالطرق التي يحددها القانون على وجود واقعة قانونية ترتبت عليها آثارها, والجريمة حتى يمكن نسبتها إلى مرتكبها يجب أن تكون هناك أدلة تثبت قيامه بالفعل؛ لأن نظرية الإثبات قامت على حقيقة مفادها هي أن الحق المجرد عن الدليل لا وجود له، ويعد عدماً عند حصول المنازعة وأن الإثبات الجنائي هو إقامة الدليل على وقوع الجريمة ونسبتها إلى فاعل معين, وهذا الدليل يكون مكون رقمي لتقديم معلومات في اشكال متنوعة مثل الأرقام والحروف والرموز والأشكال والأصوات والصور وهذا الدليل يقدم أسلوباً علمياً وقانونيا يمكن الاستعانة به في إثبات الجريمة التي تتم عبر أنظمة المعلومات الإلكترونية وكما أنه يساعد على بلورة الفهم الأكاديمي للدليل الإلكتروني المقدم لأجهزة إنفاذ وتطبيق القانون ويدعم حجية المخرجات الإلكترونية في المسائل الجزائية. وهذا الإرهاب الإلكتروني يكون من خلال استخدام التقنيات الرقمية لإخافة وإخضاع الآخرين وغالباً هذا يكون بدوافع سياسية أو عرقية أو دينية وكذلك فأنه يعتبر من أخطر أنواع الإرهاب في العصر الحاضر نظراً لاتساع نطاق استخدام التكنولوجيا الحديثة في العالم, وأن المشرع الأردني أجاز الإثبات الجزائي بكافة طرق الإثبات بشرط أن تكون وسيلة الإثبات أو أن يكون دليل قد تحصل عليه بطريقة مشروعة تطبيقاً لمبدأ الشرعية والدليل الإلكتروني ليس دليل مادي كمحضر شاهد أو غيره من الأدلة التقليدية لهذا يلجأ القضاء إلى انتداب الخبراء لإجراء عمليات الكشف والتثبت من محتوى الوثائق الإلكترونية ومن ثم تقديم التقرير الذي يعد هو البينة والدليل وليس الوثائق الإلكترونية لكنه مسلك تخافه بعض النظم القانونية عوضاً عن معارضته لأسس وأغراض إجراء الخبرة وطبيعتها كبينة تخضع للمناقشة والاعتراض والرفض والقبول.

الكلمات الدالـة: الإرهاب الإلكتروني، الدليل الإلكتروني، الإنترنت، الموقع الإلكتروني، نظام المعلومات.

المقدمة

أصبح الأمن الإلكتروني ضرورة لأن حياتنا مرتبطة ارتباطاً وثيقاً بوسائل الاتصال الحديثة التي سهلت طرق التواصل بكل أشكالها" السمعي – البصري – المكتوب " ومن هنا فإن الحفاظ على الخصوصية في حياة كل شخص أضحى من المستحيلات, لوجود ما يهدد هذه الخصوصية عن طريق ما يسمى بالإرهاب الإلكتروني فكثير من المواقع العالمية المشهورة تنصح مرتاديها والمنتسبين إليها من خطر التهديد الإلكتروني.

ولا يمكن لأي بلد في هذا العصر أن يعيش معزولاً عن التطورات التقنية المتسارعة, والآثار الاقتصادية, والاجتماعية, والأمنية الناجمة عنها, وفي ظل الترابط الوثيق بين أجزاء العالم عبر تقنيات المعلومات والاتصالات والتطبيقات التي سمحت بانسياب الأموال والسلع والخدمات والأفكار والمعلومات بين مستخدمي تلك التقنيات, بات من الضروري لكل بلد حماية أفراده ومؤسساته ومقدراته وحضارته من آثار هذا الانفتاح, ومع إدراك الجميع اليوم للفوائد الجمة لتقنية المعلومات, فإن المخاطر الكامنة في تغلل هذه التقنية في بيوتنا ومؤسساتنا تتطلب من المجتمع والدولة جميعاً الحيلولة دون حصول تلك المخاطر بشتى أنواعها.

وبالتالي فأن جريمة الإرهاب الإلكتروني تحتاج إلى أدلة لإثباتها على مرتكبها تكون من خلال تقنيات معينة تقوم بفك رموز وترجمة نبضات إلى شيء مقروء يصلح أن يكون دليل إثبات وهو ما يسمى الدليل الإلكتروني وهذا دليل يختلف عن الأدلة التقليدية والدليل الإلكتروني ومدى حجيته في الإثبات الجزائي من المواضيع المهمة بسبب تنامي وازدياد هذه الجريمة بشكل واسع في الوطن العربي ومنها الأردن واعتبار أنها من الجرائم التي تحتاج إلى معرفة واسعة فيها من قبل الضابطة العدلية والخبراء والقضاة والمحامون من أجل إثبات مدى ثبوت هذه الجريمة على مرتكبها أو عدم ثبوتها عليه ويكون ذلك من خلال أدلة إلكترونية.

---

* كلية الحقوق، الجامعة الاردنية. تاريخ استلام البحث 2018/1/17، وتاريخ قبوله 2018/9/16.

© 2019 عمادة البحث العلمي/ الجامعة الأردنية. جميع الحقوق محفوظة.

أولاً: أهمية الدراسة

تعدّ جريمة الإرهاب الإلكتروني من الجرائم صعبة الإثبات لأن التكنولوجيا لا تستطيع تحديد هوية مرتكب الجريمة الإلكترونية إلا عن طريق أجهزة معينة ووسائل إثبات تختلف عن وسائل الإثبات التقليدية لهذا فهي تتم بدهاء وبمكر ويتم استخدام تقنيات عالية فيها وقد يتم طمس معالمها ومحو آثارها قبل اكتشافها وكذلك فإن المجرم المعلوماتي يمتاز بالذكاء وبمهارة تقنية عالية ولهذا فأن الإثبات العلمي لقد تطور للكشف عن الجرائم المستحدثة ومنها جريمة الإرهاب الإلكتروني, وهذه الجريمة يتم إثباتها عن طريق أدلة رقمية وبيانات ومعلومات على الشبكة المعلوماتية (الإنترنت).

والإنترنت جعل العالم قرية صغيرة وهذا التطور التقني من صنع البشر وطبيعي أن أي تطور من صنع البشر يكون له سلبيات وإيجابيات، فقام المجرمون باستغلال هذا التطور في ارتكاب جريمة الإرهاب الإلكتروني وهذه الجريمة هي من أخطر الجرائم في العصر الحديث ولهذا فإن من واجب الدول مكافحة هذه الجريمة من خلال تطوير وسائل إثباتها لإدانة مرتكبيها ومن هذه الدول الأردن وخاصة أنها تقع في منطقة ملتهبة من الحروب والدمار والاختلاف الديني والسياسي وغيرها.

ثانياً: مشكلة الدراسة

إن هذا البحث يتناول مشكلة قانونية وهي مشكلة إثبات الجريمة بالدليل الإلكتروني بكل ما يعتريه من إشكاليات سواء فيما يخص صحة وسلامة الدليل الإلكتروني, وكذلك مدى صلاحية الأدلة المتحصلة من الوسائل الإلكترونية في الإثبات الجزائي, وكذلك تثور إشكالية بمدى السلطة التقديرية للقاضي الجزائي في تقدير الأدلة المتحصلة من الوسائل الإلكترونية في ظل مبدأ القناعة الوجدانية للقاضي الجزائي, لهذا فأن جريمة الإرهاب الإلكتروني من الجرائم الخطيرة لأنها تهدد أمن الدولة واستقرارها السياسي والاقتصادي والاجتماعي وهذه الجريمة سهل التخطيط لها وارتكابها لأنها تتم من خلال الإنترنت وتكنولوجيا المعلومات ولأهمية هذه الجريمة وتأثيرها على الدولة الأردنية فهل قوانين الجزاء الأردنية وخاصة قانون أصول المحاكمات الجزائية الأردني رقم 9 لسنة 1961 وجميع تعديلاته وقانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015م وجميع تعديلاته يستوعبان جريمة متطورة وحديثة كجريمة الإرهاب الإلكتروني وهل أدلة الإثبات التي تقدمها النيابة العامة ضد مثل هذه الجريمة فعّالة وتثبت إدانة أو براءة المتهم وهل أن هذه القوانين السابقة لا يوجد فيها ثغرات أو نواقص قد يستغلها الأشخاص الذين يقدمون على ارتكاب جرائم الإرهاب الإلكتروني وأخيراً إن رجال الضابطة العدلية والنيابة العامة في الأردن حتى تثبت جريمة الإرهاب الإلكتروني يجب أن تقدم دليل رقمي مقبول وذي مصداقية وحجية قضائية لدى المحاكم المختصة.

ثالثاً: أهداف الدراسة

1- التعرف على طرق الإثبات الجنائي لجريمة الإرهاب الإلكتروني.
2- بيان موقف المشرع الجزائي الأردني من جريمة الإرهاب الإلكتروني وإثباتها لتحقيق الردع.
3- بيان اركان جريمة الإرهاب الإلكتروني.
4- توضيح التفتيش والضبط في جريمة الإرهاب الإلكتروني.
5- توضيح ما هي الوسائل المساعدة للضابطة العدلية والنيابة العامة في إثبات جريمة الإرهاب الإلكتروني.
6- توضيح سلطة القاضي الجزائي في قبول أو تقدير الدليل الإلكتروني.
7- نشر الوعي القانوني للمجتمع والأفراد بجريمة الإرهاب الإلكتروني.

رابعاً: منهج الدراسة

سيقوم الباحث باستخدام المنهج الوصفي والتحليلي على النحو التالي:

أ) المنهج الوصفي:

من خلال وصف جرائم الإرهاب الإلكتروني وتعريفها وتعريف الدليل الإلكتروني وخصائص جريمة الإرهاب الإلكتروني وخصائص الدليل الإلكتروني وأركان جريمة الإرهاب الإلكتروني والتفتيش والضبط في جريمة الإرهاب الإلكتروني والوسائل المساعدة في إثباتها وغيرها معتمداً على المنهج الوصفي.

ب) المنهج التحليلي:

عن طريق تحليل النصوص القانونية التي تتعلق بجريمة الإرهاب الإلكتروني وإثباتها وفقاً للقانون الأردني.

خامساً: الكلمات المفتاحية :

تضمن هذا البحث بين طيات صفحاته العديد من المصطلحات والمفردات التي قد تكون للوهلة الأولى غامضة للقارئ سواء

أكان قانوني أو غيره من المهتمين بهذا الموضوع ولهذا فإنني سأوفر لها هنا بضعت أسطر لعلها تكون كافية لا زالت هذا الغموض ومن هذه المصطلحات: الإرهاب الإلكتروني، الإنترنت، الموقع الإلكتروني، الدليل الإلكتروني ونظام المعلومات.

الإرهاب الإلكتروني:– العدوان أو التخويف أو التهديد مادياً أو معنوياً باستخدام الوسائل الإلكترونية، الصادر من الدول أو الجماعات أو الأفراد على الإنسان: بدينه أو نفسه أو عرضه أو عقله أو ماله بغير حق بشتى صنوفه وصور الإفساد في الأرض.

الدليل الإلكتروني: هو الدليل المأخوذ من أجهزة الحاسوب, ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية يمكن تجميعها متنوعة مثل النصوص المكتوبة أو الصور او الأصوات أو الأشكال والرسوم.

الإثبات الجزائي: هو إقامة الدليل على صحة الادعاء أمام القاضي وفي الدعاوى الجزائية هو كل ما يؤدي إلى ثبوت وقائع الجريمة والمشتكى عليه مع انعدام الدفوع القانونية.

الإنترنت: عبارة عن ارتباط دائم بين أكثر من نظام معلومات للحصول على البيانات وتبادلها.

الموقع الإلكتروني: عبارة عن مكان إتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدد.

نظام المعلومات: عبارة عن مجموعة من البرامج والأدوات المعدة لإنشاء البيانات أو المعلومات إلكترونياً أو إرسالها أو تسلمها أو معالجتها أو تخزينها أو إدارتها.

المبحث الأول:

التفتيش والضبط والوسائل المساعدة في الإثبات:–

جرائم الإرهاب الإلكتروني هي من الجرائم النظيفة وذلك لصعوبة اكتشاف دليل ثبوتها؛ فلا أثر فيها لأية عنف أو دماء ,وإنما مجرد أرقام وبيانات يتم تغييرها أو محوها من السجلات المخزونة في ذاكرة الحاسبات الآلية وليس لها أثر خارجي مادي, وهناك صعوبات تواجه كافة أطراف المنظومة الأمنية والقضائية, وهي تتجلى عندما تكون الجريمة واقعة على برامج الكمبيوتر وبياناته أو بواسطتها, وذلك بالنظر إلى قلة الآثار المادية التي قد تنتج عن هذا النوع من الجرائم, وكثرة عدد الأشخاص الذين قد يترددون على مسرح الجريمة خلال المدة الفاصلة بين وقوع الجريمة والكشف عنها.

وهذه جريمة الإرهاب الإلكتروني هي كالجرائم التقليدية الأخرى وتتضمن إجراءات التفتيش والضبط والتحقيق لأنها تمس حقوق الناس وحرياتهم لهذا يجب أن تكون الإجراءات التي يتم تطبيقها قانونية لأن أي إجراء غير قانوني يؤدي إلى بطلان جميع الإجراءات وقد أكد المشرع الأردني في قانون الجرائم الإلكترونية رقم (27) لسنة 2015م على وسائل الإثبات وخاصة التفتيش والضبط والتحقيق.

ولهذا سيقسم هذا المبحث إلى مطلبين:–

المطلب الأول:– التفتيش والضبط

المطلب الثاني:– الوسائل المساعدة في الإثبات

المطلب الأول: التفتيش والضبط:–

قد يتطلب الأمر في كثير من الأحيان ولوج البيئة المعلوماتية بحثاً عن الدليل وكشف مرتكبي الجرائم المعلوماتية لإيقاع العقوبات عليهم, وتكمن صعوبة كشف الدليل باتصاف المجرم المعلوماتي في الغالب بالذكاء والخبرة الواسعة مقارنة بنظيره المجرم التقليدي وعدم تركه لأي أثر خارجي بصورة مرئية بحيث يستطيع المجرم الإلكتروني تدمير دليل الإدانة في وقت قياسي الذي من شأنه إعاقة مهمة أجهزة الاستدلال والتحقيق في الوصول إلى الدليل, والنيابة العامة هي السلطة المختصة بالتفتيش والضبط ومن يساعدها من رجال الضابطة العدلية وأن التفتيش هي مرحلة سابقة لضبط الأشياء المتعلقة بالجريمة في أثناء التفتيش وكل ذلك حتى يتم إثبات ارتكاب جريمة الإرهاب الإلكتروني.

الفرع الأول: التفتيش:–

الأحكام الإجرائية هي القواعد التي تبين الأوضاع والإجراءات اللازم إتباعها أو السبيل الواجب سلوكه عند تطبيق القاعدة الموضوعية لاقتضاء الحقوق التي تقررها هذه القواعد, والتفتيش هو عبارة عن إجراء من إجراءات التحقيق التي تهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة المسكن أو الشخص وذلك بهدف إثبات ارتكابها أو نسبتها إلى المتهم وفقاً لإجراءات قانونية محددة[1].

والتفتيش يعتبر من أهم إجراءات التحقيق الابتدائي لأنه قد يؤدي إلى ضبط الأشياء المتعلقة بالجريمة إذ قد تكون أداة ارتكابها

أو موضوعها أو متحصلاً عنها وأما بالنسبة للتفتيش في الجرائم الإلكترونية وخاصة جريمة الإرهاب الإلكتروني يتطلب مهارات فنية عالية في المحقق حتى يتمكن من جمع الأدلة وعدم إضاعتها وسرعة إيجادها[2].

والنيابة العامة في الأردن هي من تقوم بإجراء التفتيش بعد الحصول على إذن المدعي العام المختص, فالضابطة العدلية هي من تقوم بتفتيش الأجهزة الإلكترونية والبرامج وأي شيء من نظام المعلومات يتعلق بارتكاب جريمة الإرهاب الإلكتروني من أجل إيجاد دليل إثبات ضد الجاني بشرط الحصول على موافقة من المدعي العام المختص أو المحكمة المختصة وتلزم الموظف أن ينظم محضراً بالإجراءات والأعمال التي قام بها ويوقعه ويقدمه إلى المدعي العام المختص أو المحكمة المختصة وبما أن قانون الجرائم الإلكترونية الأردني لم يحدد آلية التفتيش فيتم الرجوع إلى القواعد العامة في التفتيش في قانون أصول المحاكمات الجزائية الأردني رقم (9) لسنة 1961 في المواد 81-92.[3].

وتخضع مكونات الحاسوب المادية والمعنوية وشبكات الحاسوب للتفتيش وهي على النحو التالي:-

أ- خضوع مكونات الحاسوب المادية للتفتيش:

الحاسوب يتكوّن من مجموعة من الوحدات ولكل منها وظيفة محددة وتتصل مع بعضها بعضاً بشكل يجعلها تعمل كنظام متكامل مثل الشاشة ولوحة المفاتيح ووحدة الذاكرة ووحدة التحكم ووحدة الإخراج، فجميع الوحدات تشكل الحاسوب لأنه يتكون من مجموعة من الدوائر الحسابية والمنطقية والسجلات التي تقبل إدخال البرامج وتنسيق وتبادل البيانات والأوامر [4].

ولا يواجه صعوبة من يفتش المكونات المادية للحاسوب لأنها واضحة على وقوع الجريمة ونسبتها لشخص معين، فيقومون بعد ذلك بوضع الأختام وضبط الأدلة وإخبار النيابة العامة[5] وقد يتم تفتيش المكونات المادية للحاسوب وهو يكون وفق المكان الموجود فيه وهو يخضع لإجراءات التفتيش العادية، فإذا كان مكان خاص فله حالات محددة بدخول المساكن، إما مكان عام، فينطبق عليه تفتيش الأشخاص لأن هناك شخص هو الذي يحمل جهاز الحاسوب أو الهاتف أو اي وسيلة إلكترونية[6].

ب- خضوع مكونات الحاسوب المعنوية للتفتيش:-

تفتيش البيانات المخزنة التي جرى التلاعب فيها أو تغييرها وتفتيش نظام المعلومات والبرامج لتأكد من ارتكاب جريمة الإرهاب الإلكتروني ويتم تقديم البرامج غير المشروعة المخزنة على الحاسوب الخاص بالمتهم كدليل اتهام ضده أمام المحكمة المختصة.

وقد يمتد التفتيش للجهاز الإلكتروني للمتهم وإلى سجلات البيانات الموجودة في موقع آخر بشرط أن تكون البيانات الخاصة ضرورية لإظهار الحقيقة[7]. ويمكن ضبط هذه البيانات وتسجيلها على الورق أو على الأقراص أو على أية دعامة أخرى، بحيث تصلح دليل إدانة أو براءة للمتهم, والتفتيش عن البيانات المخزنة آلياً يتم عن طريق القيام بعملية ولوج للأنظمة المعلوماتية التي تحويها لضبط ما يعد صالحاً من هذه البيانات كدليل أو قرينة لارتكاب جريمة ما[8].

ج- خضوع شبكات الحاسوب للتفتيش:-

شبكات الحاسوب هي مجموعة مكونة من اثنين أو أكثر من أجهزة الحاسوب والمتصلة ببعضها اتصالاً سلكياً أو لا سلكياً والشبكات الواسعة ترتبط من أماكن متفرقة وبعيدة ولهذا فأن إجراءات التفتيش الفنية تتطلب وجود وسائل فنية متطورة للتفتيش على شبكات الحاسوب والمراقبة الإلكترونية لنظم المعلومات والشبكات المعلوماتية ورغم أنها تتعارض مع الحريات العامة إلا أن الموازنة بين مكافحة جرائم الإرهاب الإلكتروني وتقديم أدلة على ارتكابها والحريات العامة فتكون المصلحة العامة أولى بالحماية من المصلحة الخاصة ولهذا هناك أجهزة تلتقط وتراقب الاتصالات والبيانات والمعلومات على الإنترنت بحيث أصبحت جميع وسائل الاتصال الحديثة مراقبة[9].

ولتفتيش الأجهزة الإلكترونية ونظام المعلومات وغيرها حتى يتم جمع الأدلة التي تثبت وقوع جريمة الإرهاب الإلكتروني يتطلب تحقق عدة شروط بعد الحصول على إذن النيابة العامة بالتفتيش وهي:-

أ) وقوع جريمة معلوماتية: وهي كل فعل غير مشروع مرتبط باستخدام الحاسوب لتحقيق أغراض غير مشروعة[10].

ب) ارتكاب شخص أو عدة أشخاص الجريمة المعلوماتية (الإرهاب الإلكتروني).

ج) يوجد قرائن تدل على وجود أجهزة ومعدات تقنية لدى المتهم، بأن يكون لدى رجال الضابطة العدلية أسباب جدية بأنه ارتكب جريمة معلوماتية.

د) محل التفتيش هو الحاسوب بمكوناته المادية والمعنوية وشبكات الاتصال به وتفتيش مستخدم الحاسوب كذلك[11].

يرى الباحث أن قانون الجرائم الإلكترونية الأردني رقم (27) لسنة 2015 قد أعطى النيابة العامة سلطة واسعة في التفتيش وفق القواعد العامة وبالتالي يجوز تفتيش مكونات الحاسوب المادية والمعنوية وشبكات الحاسوب وأن يمتد التفتيش لجهاز حاسوب

موجود في مكان آخر مرتبط بنهاية طرفية متصلة بجهاز حاسوب المتهم.

الفرع الثاني: الضبط :

الضبط هو وضع اليد على اي شيء يتصل بالجريمة التي وقعت من أجل الكشف عن الحقيقة وعن مرتكبيها وأن الهدف الذي تسعى له النيابة العامة من التفتيش هو ضبط الأدلة والوثائق وأي شيء تساعد في الكشف عن الجريمة, وإن ضبط الأدلة الإلكترونية في جريمة الإرهاب الإلكتروني يتطلب ضبط المكونات المادية والمكونات المعنوية والبرمجيات لأنظمة الحاسوب وضبط المعطيات التي تنتقل في شبكة المعلومات لأنها تربط الحواسيب ببعضها وما يتصل بها[12].

والمضبوطات التي ينظم المدعي العام محضراً فيها تنطبق على ضبط الأشياء المادية بالنسبة لمكونات الحاسوب ويشمل أيضاً البيانات التي تحتويها دعامة مادية كالأقراص الصلبة والمضغوطة أما البيانات ككيان معنوي غير ملموس فإنها لا تكون محلاً للضبط وفق هاتين المادتين[13].

ولقد انقسم الفقه إلى اتجاهين يرى البعض أن بيانات الحاسوب لا تصلح لأن تكون محلاً للضبط لعدم وجود الكيان المادي ولا يمكن ضبطها إلا إذا تم نقلها على كيان مادي مثل القيام بتصويرها أو نقلها على دعامة مادية أو أي وسيلة مادية وحجة هذا الرأي أن النصوص التشريعية العامة التي تتعلق بالضبط تنطبق على الأشياء المادية فقط، أما الاتجاه الثاني أن البيانات الإلكترونية هي عبارة عن موجات كهرومغناطيسية أو ذبذبات إلكترونية ويمكن تسجيلها وتخزينها وحفظها على أشياء مادية وبالتالي يمكن نقلها واستقبالها فوجودها المادي لا يمكن إنكاره[14].

فالمشرع الأردني منح موظفي الضابطة العدلية ضبط المكونات المادية والمعنوية للحاسب الآلي وهذا يظهر من كلمات "الأجهزة والأدوات والبرامج وأنظمة التشغيل..." وبالتالي يظهر أن المشرع الأردني قد حسم الخلاف الفقهي حول ضبط المكونات المعنوية للحاسب الآلي بأن أجاز بصريح المادة ضبط المكونات المعنوية والمادية للحاسب الآلي وكذلك أنه يمكن التحفظ على المعلومات والبيانات المتعلقة بارتكاب الجريمة حيث أنه يتم التحفظ على الأدلة داخل جهاز الحاسوب من خلال حجز الحاسوب والدليل الموجود فيه إما حفظ الأدلة في الإنترنت فهي غالباً تحتاج إلى خبير فني يرصد موقع الإنترنت أو المعلومات التي تشير إلى الجريمة مثل جريمة الإرهاب الإلكتروني والخبير دائماً يلجأ إلى ذاكرة الخادم الذي يربط العالم الرقمي أو إخراج الأدلة الرقمية إلى العالم المادي وهذه الأدلة المادية أو المعنوية تخضع للسلطة التقديرية للقاضي[15] والمشرع الأردني جعل الحكم بالمصادرة من صلاحيات المحكمة المختصة وهي تصادر الأجهزة التي ضبطتها الضابطة العدلية أو تأمرهم بضبط أمور أخرى ذات علاقة بالجريمة المرتكبة وهي هنا جريمة الإرهاب الإلكتروني وكذلك أن هناك صلاحية للمحكمة المختصة بتوقيف أو تعطيل عمل نظام معلوماتي أو موقع إلكتروني استخدام لارتكاب الجريمة الإلكترونية[16].

والأشياء التي يمكن ضبطها من الحاسوب أو المرتبطة به هي:-

أ) جهاز الحاسوب، المكون من الشاشة ولوحة المفاتيح والسماعات والفأرة وغيرها من المعدات.

ب) قرص التخزين الثابت وأقراص الليزر والأقراص المرنة.

ج) الأشرطة الممغنطة.

د) الأوراق التي تمت طباعتها والمحفوظة في الملفات.

هـ) لوحة الأم ولوحة الدوائر والطابعة.

يرى الباحث أن قانون الجرائم الإلكترونية الأردني رقم (27) لسنة 2015 قد حسم الخلاف الفقهي وأجاز ضبط ومصادرة المكونات المادية والمعنوية للحاسب الآلي وكل ذلك تحت رقابة من المحكمة المختصة بذلك لأن المواد المتعلقة بالضبط في قانون أصول المحاكمات الجزائية الأردني واقد تنطبق على ضبط الأشياء المادية للحاسوب دون البيانات والكيان المعنوي للحاسوب.

المطلب الثاني:- الوسائل المساعدة في الإثبات:

النيابة العامة في الأردن تعتمد أساليب متعددة في التحقيق في الجرائم الإلكترونية وهذه الوسائل قد تكون مادية ومعنوية ليستخدمها المدعي العام في تنفيذ التحقيق لأن التحقيق في الجرائم الإلكترونية يحتاج إلى معرفة تامة وإدراك لوسائل تثبت وقوع الجريمة والوصول إلى الجاني ونسبتها إليه[17].

وتنقسم الوسائل المساعدة في إثبات جريمة الإرهاب الإلكتروني إلى فرعين:

الفرع الأول: الوسائل الإجرائية:

هي تلك الإجراءات التي تستعمل في أثناء تنفيذ طرق التحقيق الثابتة والمحددة والأساليب المتغيرة وغير المحددة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبها.

1- التأكد من وقوع الجريمة:

توافر المعلومات المنشورة من خلال شبكة الإنترنت قد تظهر انتشار الفيروسات أو وقوع عمليات اختراق أو قرصنة عند وصول الجهة الأمنية بلاغاً عن جريمة ما ثم يقوم رجال الضابطة العدلية بالإجراءات التي تتبع تلقي البلاغ من التأكد من صحة البلاغ والتحفظ على مكان الجريمة وتأمينه وتحديد أطراف الجريمة وكل من له صلة بها وحصر الشهود ومنع مغادرتهم وحصر الأدلة ورفع الاثار ويجب أن يتم إظهار الحقائق في مرحلة جمع الاستدلالات وإثباتها في محضر نظراً لأهميتها في تحديد الجريمة ورسم خطوات البحث المجهول[18]، من خلال التثبت من توافر أركان الجريمة وتحديد مكان الجريمة ووصفه[19]، ووقت وقوع الجريمة[20]، ومعرفة كيفية ارتكاب الجريمة[21]، ومعرفة الظروف المحيطة بالجريمة، ومعرفة أسباب وقوع الجريمة[22].

2- اقتفاء الأثر:

أخطر ما يخشاه المجرم الإلكتروني تقصي أثره في أثناء ارتكابه للجريمة[23]، أن المخترقين أول ما يقوم به هو مسح آثاره حتى لا يتم القبض عليه ويتم تقصي الدليل عن طريق بريد إلكتروني تم استقباله أو عن طريق تتبع الأثر للجهاز الذي تم استخدامه للقيام بعملية الاختراق وفي أحد المواقع المتخصصة في أمن المعلومات في الإنترنت تتطرق إلى قصص تعرض المواقع لعمليات اختراق وكيف تم تتبع أثر المخترق والتحكم بجهازه[24].

3- الاستعانة بالذكاء الصناعي:

جمع الأدلة الجنائية في جرائم الإلكترونية تعتمد في نجاحها على تقنيات الحاسوب في تحليل القرائن واستنتاج الحقائق وعلى حصر الحقائق والاحتمالات والأسباب والفرضيات، وبعد ذلك يتم معرفة النتائج على ضوء معاملات حسابية يتم تحليلها بالحاسوب وفق برامج صممت خصيصاً لهذا الغرض، تعتمد على نظرية الاحتمالات بإعطاء كافة الاحتمالات ثم أكثر الاحتمالات وصولاً ثم الاحتمال الأقوى مع إعطاء الأسباب[25].

الفرع الثاني: الوسائل المادية:

الأدوات الفنية هي التي تستخدم في بيئة نظم المعلومات التي يمكن من خلالها أن يتم تنفيذ إجراءات وأساليب التحقيق المختلفة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبيها من الوسائل المادية المستخدمة، بالتالي أنه يجب التركيز على الجرائم التي ترتكب عن طريق شبكة الإنترنت وعلى الرغم أن الشبكات الأخرى لها نفس الخصائص[26].

1- أدوات الضبط:

تحتاج الضابطة العدلية إلى ضبط الجريمة وإثبات وقوعها والمحافظة على الأدلة حتى نسبتها إلى الجاني لتقديمها إلى النيابة العامة وبدورها النيابة العامة تقدم الأدلة إلى المحكمة المختصة ولهذا يوجد أدوات تقوم بضبط الجريمة كغالبية برامج الحماية وأدوات المراجعة وأدوات مراقبة المستخدمين للشبكة وأدوات التنصت على الشبكة والتقارير التي تنتجها نظم أمن البيانات ومراجعة قاعدة البيانات وبرامج النسخ الاحتياطي والتسجيل وأدوات الضبط الأخرى IDS MNM Windows Conten Management كما يمكن استخدام أغلب الأدوات المستخدمة في الجريمة كأداة ضبط مثل أدوات جمع المعلومات عن الزائرين للموقع كبرمجيات Jana Appletsأو Cookies والبرامج الأخرى[27].

2- عناوين الإنترنت (البريد الإلكتروني وبرامج المحادثة):

عنوان الإنترنت هو المسؤول عن تراسل حزم البيانات عبر الإنترنت وتوجيهها إلى أهدافها، وهو يتيح للموجهات والشبكات المعنية بنقل الرسالة ويوجد عنوان (IP) بكل جهاز مرتبط بالإنترنت ويتكون من اربعة أجزاء، والجزء الواحد له ثلاث خانات فيكون المجموع أثني عشر فإنه كحد أقصى، حيث يشير الجزء الأول من اليسار إلى المنطقة الجغرافية والجزء الثاني لمزود الخدمة لمجموعة الحواسيب المرتبطة والرابع يحدد الحاسوب الذي تم الاتصال منه[28].

والنيابة العامة أول شيء تقوم به لإثبات الجريمة هو البحث عن رقم الجهاز وتحديد موقعه لمعرفة الجاني الذي يقوم بجريمة الإرهاب الإلكتروني ويمكن لمزود خدمة الإنترنت أن تراقب المشترك مثل شركة زين أو أورانج أو أمنية, هنالك العديد من الطرق لمعرفة عنوان (IP) الخاص بجهاز الحاسوب في حال الوصول المباشر مثل حالة العمل على نظام التشغيل Windows بكتابة Winipcfg في أمر التشغيل ليظهر مربع حوار يبين فيه عنوان (IP) وهذا عنوان يتغير كلما تم الاتصال بالإنترنت مرة أخرى

وأنه في حالة استخدام أحد برامج المحادثة كأداة للجريمة فإنه يتطلب تحديد هوية المتصل وتحدد رسالة البريد الإلكتروني عنوان شخصية مرسلها حتى لو لم يدون معلوماته في خانة المرسل، شرط أن تكون المعلومات التي وضعت في مرحلة إعدادات البريد الإلكتروني معلومات صحيحة[29].

3- البروكسي (Proxy):

البروكسي هو وسيط بين الشبكة ومستخدمها بحيث أن تضمن الشركات الكبرى المقدمة لخدمة الاتصال بالشبكات قدرتها لإدارة الشبكة وضمان الأمن وتوفير خدمات الذاكرة الجاهزة Cache Memory حيث يتلقى مزود البروكسي عبر الإنترنت طلباً من المستخدم بحيث يبحث عن الصفحة المطلوبة ضمن ذاكرة كاشي Cache المحلية المتوافرة فيتحقق البروكسي فيما إذا كانت هذه الصفحة قد جرى إنزالها من قبل، فإذا كانت كذلك بالفعل أعادها إلى المستخدم دون الحاجة إلى إرسال الطلب إلى الشركة العالمية أما إذا لم يجد مزود البروكسي الصفحة المطلوبة ضمن ذاكرة كاشي، فإنه يعمل كمزود زبون ويرسل الطلب إلى الشبكة العالمية بحيث يستخدم أحد عناوين (IP)، وأهم مزايا مزود البروكسي أن ذاكرة كاشي المتوافرة لديه، يمكن أن تحتفظ بتلك العمليات التي تمت عليها، مما يجعل دورها قوياً في الإثبات عن طريق فحص تلك العمليات المحفوظة بها، التي تخص المتهم والموجودة عند مزود الخدمة[30].

4- برامج التتبع:

تقوم هذه البرامج بالتعرف على من يقوم بالاختراق وإشعار الجهة المتضررة بعملية الاختراق مثال برنامج Hack Tracer وهو مصمم للعمل في الأجهزة المكتبية وعندما يرصد محاولة اختراق للحاسوب يعمل بسرعة على إغلاق منافذ الدخول أمام المخترق ثم يبدأ في عملية مطاردة حتى يقوم باقتفاء أثر مرتكب عملية الاختراق والجهاز الذي حدثت من خلال العملية[31].

بناءً على ما سبق فأن البرنامج يتكون من شاشة رئيسية تظهر للمستخدم بياناً شاملاً بعملية الاختراق التي حدثت وتحمل اسم الحدث وتاريخ حدوثه وعنوان (IP) الذي تمت من خلاله واسم الشركة المزودة لخدمة الإنترنت وأرقام مداخلها ومخارجها ومعلومات أخرى، أن أي محاولة اختراق تظهر شاشة أخرى صغيرة مع تحذير صوتي يظهر على الشاشة عنوان (IP) الخاص به ويمكن للمستخدم الاختيار ما بين أربعة أوامر موجودة في هذه الشاشة الفرعية منه، والأمر الثاني هو Trace It وبمجرد الضغط على هذا الأمر تظهر شاشة أخرى وعليها اسم الدولة التي تم الاختراق منها ثم الضغط على NEXT حتى يستكمل عملية اقتفاء الأثر ثم تظهر شاشة ثالثة عليها خريطة العالم وخط طويل ممتد من المدينة التي تمت منها محاولة الاختراق إلى المدينة التي يقيم فيها المستخدم ويوجد أسفل الخريطة مجموعة من الأوامر في Map وبالضغط عليها تظهر خريطة عليها خط سير محاولة الاختراق[32].

يرى الباحث أن قانون الجرائم الإلكترونية الأردني رقم (27) لسنة 2015 وكذلك وفقاً للقواعد العامة الجزائية بأنه يتم الإثبات الجنائي بكافة طرق الإثبات ومنها جريمة الإرهاب الإلكتروني ولأهمية جريمة الإرهاب الإلكتروني وتميزها عن غيرها من الجرائم فتحتاج إلى وسائل إثبات حديثة تكون بنفس مواصفات وتميز طريقة ارتكاب هذه الجريمة ولهذا فإن الوسائل المساعدة في الإثبات التي تطرقنا إليها سواء الوسائل المادية أو الإجرائية هي داعم وشريك حقيقي لرجال الضابطة العدلية والمحكمة المختصة في إثبات جريمة الإرهاب الإلكتروني.

المبحث الثاني :

اقتناع القاضي الجزائي بالدليل الإلكتروني

الدليل الإلكتروني هو تطبيق من تطبيقات الدليل العلمي ويتميز بالموضوعية والحياد والكفاءة وهو محكم وفق قواعد علمية حسابية قاطعة لا تقبل التأويل مما يقوي يقينيته, ويساعد القاضي على التقليل من الأخطاء القضائية والاقتراب من العدالة بخطوات أوسع, والتوصل إلى درجة أكبر نحو الحقيقة, وهو دليل حديث في الإثبات الجنائي أمام القضاء, فهل يعتبر هذا الدليل حاسم بالنسبة للقاضي الجزائي أو ما زال هناك سلطة تقديرية للقاضي الجنائي في قبول الدليل الإلكتروني أو تقدير الدليل الإلكتروني.

وتعد مرحلة المحاكمة من أهم المراحل لأنه مرحلة الجزم بتوافر الدليل أو أدلة يقتنع بها القاضي لإدانة المتهم, ومع أن الأدلة ليست سوى وسائل تستهدف للتوصل للحقيقة ويمكن من حيث المبدأ إقامتها أمام القضاء الجزائي وتأسيس اقتناع القاضي عليها ما دامت مشروعة, إلا أن قبول ما يكون منها ناشئاً أو مستمداً من نظم المعالجة الآلية قد ترهب القاضي الجزائي, ذلك أن

مستودع هذه الأدلة هو الوسائل الإلكترونية.

وسيقسم هذا المبحث إلى مطلبين:-

المطلب الأول:- سلطة القاضي في قبول الدليل الإلكتروني

المطلب الثاني:- سلطة القاضي في تقدير الدليل الإلكتروني

المطلب الأول:- سلطة القاضي في قبول الدليل الإلكتروني

طبيعة نظام الإثبات في أي دولة هو المعيار الذي يتحدد على أساسه موقف القوانين المقارنة بالنسبة لسلطة القاضي الجزائي في قبول الدليل الإلكتروني[33]، وإن المشرع الأردني أجاز للقاضي الجزائي الاستناد إلى الدليل الإلكتروني لإثبات الفعل الجزائي تطبيقاً لمبدأ حرية الإثبات الجنائي, لأن هذا المبدأ يمثل لب نظم الإثبات الحر.

ولهذا يجوز للقاضي الجزائي الاستناد إلى الدليل الإلكتروني لإثبات الفعل الجزائي في جرائم تقنية المعلومات, وهذا ما سيتم تقسيمه في هذا المطلب إلى فرعين:

الفرع الأول: مبدأ حرية الإثبات الجزائي كأساس لقبول الدليل الإلكتروني

الفرع الثاني: النتائج التي تترتب على حرية الإثبات الجزائي

الفرع الأول: مبدأ حرية الإثبات الجزائي كأساس لقبول الدليل الإلكتروني:

حرية الإثبات الجنائي هي من المبادئ المستقرة في نظرية الإثبات الجزائي ويعني هذا المبدأ هو جواز لجوء جميع الأطراف إلى اي وسيلة إثبات يريدونها للتدليل على صحة ما يدعونه ومن جهة أخرى تستطيع النيابة العامة أن تلجأ إلى أي وسيلة إثبات لإدانة المتهم وأن القاضي هو يوازن هذه الأدلة وأيها أقوى من الآخر تبعاً للسلطة التقديرية الممنوحة له[34].

ولقد أكد قانون العقوبات الأردني وقانون أصول المحاكمات الجزائية الأردني في المادة 147 على حرية الإثبات الجنائي وهذا مستمد من القواعد العامة في الإثبات الجنائي أما القوانين الخاصة مثل قانون الجرائم الإلكترونية الأردني رقم (27) لسنة 2015م الذين تضمن موضوع الإرهاب الإلكتروني فلم ينص على الإثبات الإلكتروني وبالتالي فإن الدليل الإلكتروني هو مقبول في الإثبات الجنائي من حيث الأصل العام.

وقد أكدت محكمة التمييز الأردنية على ذلك بقولها: أن المادة 147 من قانون أصول المحاكمات الجزائية أعطت محكمة الموضوع الحق بأن تأخذ من الأدلة المقدمة في الدعوى ما تقنع به ويطمئن إليه ضميرها ووجدانها وعليه وحيث أن محكمة الجنايات الكبرى وجدت أن بينات النيابة كافية لتجريم المتهمين بالجرم المسند إليهم فإن عدم أخذها بالبينة الدفاعية هو من صلاحياتها ولا معقب عليها من محكمة التمييز ما دام إن الأخذ بالبينة الدفاعية من عدمه تستقل بها محكمة الموضوع وهي غير ملزمة بيان سبب عدم أخذها بالبينة الدفاعية ويكون القول بغير ذلك مستوجب الرد[35].

الفرع الثاني: النتائج التي ترتب على حرية الإثبات الجزائي:

إن إعمال مبدأ حرية الإثبات على النحو السابق ذكره يجعل القاضي الجزائي يتمتع بسلطة تقديرية واسعة حيث له سلطة أوسع من القاضي المدني، وتأتي هذه السلطة من طبيعة الجرائم الجنائية التي تتطلب قناعة وجدانية من القاضي وتقديره وقبول وترجيح هذا الدليل دون غيره من الأدلة.

والقاضي الجزائي قد يطلب أدلة الإلكترونية على ثبوت قيام المتهم بارتكاب جريمة الإرهاب الإلكتروني من النيابة العامة الملزمة بإقامة الدليل ضده أو قد يطلب دليل الإلكتروني من المتهم ينفي مسؤوليته ثم تكون قناعه القاضي هي الفاصل في الحكم بناءً على الدليل الإلكتروني الأقوى الذي يقتنع به, ودور القاضي له عدة جوانب:

أولاً: الدور الإيجابي للقاضي بتوفير الدليل الإلكتروني:

يقصد بالدور الإيجابي للقاضي الجزائي في توفير الدليل الإلكتروني هو عدم التزام القاضي بما يقدمه له أطراف الدعوى من أدلة وإنما له سلطة بل وواجب عليه أن يبادر من تلقاء نفسه إلى اتخاذ جميع الإجراءات لتحقيق الدعوى والكشف عن الحقيقة الفعلية فيها، لذلك أن الحقيقة لا تظهر من تلقاء نفسها وإنما في حاجة دوماً إلى من يبحث وينقب عنها وليس له أن يقتنع بما يقدمه إليه أطراف الدعوى وإنما عليه أن يبحث بنفسه عمّا يعتقد أنه مفيد في إظهار واكتشاف الحقيقة في كل نطاقها ذلك أن الضرر الذي تحدثه الجريمة ليس ضرراً فردياً فحسب وإنما أضحى ضرراً عاماً يهدد مصلحة المجتمع في أمنه واستقراره وسلامته، لذلك كان من الضروري تسليح القاضي بالسلطات التي تمكنه من الوصول إلى الحقيقة الفعلية في الدعوى المنظورة أمامه[36][37].

والنيابة العامة في الأردن عليها أن تقيم الدليل على المتهم بالإدانة والمتهم عليه أن ينفي هذا الدليل بكل الإمكانيات المخولة

له ولكن يتدخل القاضي الجنائي لأن دوره ليس دور سلبي كالقاضي المدني الذي (يقتصر على الموازنة بين الأدلة التي يقدمها الأطراف ويرجح إحداهما) ولهذا فالقاضي الجزائي يكون له دور إيجابي يبحث عن الأدلة بهدف الوصول إلى الحقيقة عن طريق اتخاذ أي إجراء يراه مناسب والقاضي الجزائي له حرية الاقتناع ,وبالتالي فإن للقاضي الجزائي سواء بناءً على طلبات الأطراف أو بموجب مقتضيات وظيفته, أن يأمر باتخاذ الإجراء الذي يراه مناسباً وضرورياً للفصل في القضية وفق القانون والعدالة.

وتطبيقاً على جرائم الإلكترونية, فإن القاضي الجزائي يستطيع من أجل الوصول إلى الحقيقة أن يوجه أمراً إلى مزود الخدمة بتقديم المعطيات التي تسمح بتعرف المرسل إليه أو المرسل إليهم الاتصال وكذلك عناوين المواقع المطلع عليها, وهنالك جهات مختصة بالأدلة الإلكترونية يجب عليها أن تقدم له معطيات وأدلة تثبت ارتكاب المتهم جريمة الإرهاب الإلكتروني ويوجد في الأردن وحدة تابعة للبحث الجنائي وتسمى وحدة مكافحة الجرائم الإلكترونية، وقد يطلب القاضي تتبع الاتصالات السلكية واللاسلكية إذا وجد أنه إجراء ملائم ويتعلق بالقضية التي ينظرها[38].

وللقاضي الجزائي أن يستعين بخبراء في المجال الإلكتروني لتوضيح بعض الأمور أو لتقديم تقارير منهم عن أمور معينة يرى أنها مهمة, وهؤلاء الخبراء لهم الدور الكبير في مساعدة القضاء للفصل في القضايا, وأن استعانة القاضي بالخبير لا يعني أن الخبير هو الذي يحكم ويفصل في القضية بل على العكس فإن القاضي يعتبر هو الخبير الأعلى وهو الذي يقيم الخبير والدليل وبناءً على ذلك يقوم بإصدار حكمه على القضية بالإدانة أو البراءة.

ثانياً: الدور الإيجابي للقاضي في قبول الدليل الإلكتروني:

أهم مرحلة وهي البحث عن الدليل وتقديمه سواء من النيابة العامة أو المتهم أو القاضي ثم تصبح مرحلة قبول الدليل الإلكتروني وأن مبدأ المشروعية الجزائية تتطلب أن يكون الدليل الإلكتروني المستخرج مقبول ومشروع في الإثبات الجزائي لأن القاضي لا يحكم إلا على الدليل المشروع بأن تم البحث عنه والحصول عليه وفقاً لمبدأ المشروعية.

يرى الباحث أن سلطة القاضي الجزائي في قبول الدليل الإلكتروني في الأردن قائمة على حرية الإثبات الجنائي لذلك فإن مسألة قبول الدليل الإلكتروني لا تثير أي إشكالية قانونية بأنها تخضع للسلطة التقديرية القاضي.

المطلب الثاني:- سلطة القاضي في تقدير الدليل الإلكتروني:

هناك مبدأ أساسي وجوهري في الجزاء وهو أن سلطة القاضي في تقدير الدليل بشكلٍ عام والدليل الإلكتروني بشكلٍ خاص هو حرية الإثبات وحرية القاضي تقدير الأدلة وفقاً لقناعته الشخصية, إلا أنه في الوقت الذي منح فيه القاضي الجزائي حرية واسعة في مجال تقدير الأدلة وفقاً لاقتناعه الشخصي, أحاطه بسياج من القيود والضوابط التي تشكل في مجموعها شروطاً لإعمال المبدأ بل وتطبيقه التطبيق الأمثل بما يضمن الوصول إلى الحقيقة الفعلية في الدعوى ومع المحافظة على الحقوق والحريات.

وبناءً على ما سبق فأن قبول الدليل الإلكتروني في الإثبات الجزائي بصفة عامة, والإثبات في مجال الجرائم الإلكترونية وخاصة في الإرهاب الإلكتروني يقوم على أساس مبدأ حرية الإثبات والاقتناع, وبالتالي يترتب على ذلك هو خضوعه لحرية تقدير القاضي الجزائي, ولهذا سيقسم هذا المطلب إلى فرعين:

الفرع الأول: اقتناع القاضي الجزائي ودوره في تقدير الدليل الإلكتروني

الفرع الثاني: ضوابط اقتناع القاضي بالدليل الإلكتروني

الفرع الأول: اقتناع القاضي الجزائي ودوره في تقدير الدليل الإلكتروني:

الدليل الإلكتروني يخضع للمبدأ العام في الإثبات الجزائي وهو بأن للقاضي الجزائي الحرية في الاقتناع وفقاً لقناعته الشخصية بالنسبة للدليل الإلكتروني ولم يتضمن قانون الجرائم الإلكترونية الأردني أي نص يقيد تقدير القاضي للدليل الإلكتروني وبالتالي فالقاضي يملك حرية واسعة في تقدير أدلة الإثبات ووزن الأدلة وتقديرها حتى يكون قناعة تامة في القضية ويحكم على المتهم الإدانة أو البراءة.

وسيتم تناول هذا المبدأ على الترتيب التالي:

أولاً: مفهوم مبدأ حرية اقتناع القاضي:

يعد مبدأ الاقتناع القضائي أحد المبادئ التي تقوم عليها نظرية الإثبات في المواد الجزائية وعنه تتفرع معظم القواعد التي تحكم هذا الإثبات[39]، وقد كانت هناك العديد من الآراء بالنسبة لتوضيح مدلوله[40] وهي بمعنى واحد: أن للقاضي أن يستمد تكوين اعتقاده من اي دليل تطمئن إليه نفسه ويسكن إليه وجدانه، من دون أي قيد يقيده في ذلك سواء من تلك الأدلة التي طرحت عليه من قبل النيابة العامة أو الخصوم أو التي يرى بنفسه تقديمها وهذه الحرية التي يتمتع بها القاضي الجزائي في هذا المجال ليست

مقررة بهدف توسيع الإدانة أو البراءة، وإنما هي مقررة له بالنظر إلى صعوبة الحصول على الدليل في المواد الجزائية[41] وأن الاقتناع القاضي وخاصة لدى المحاكم الجزائية والقاضي الجزائي لقد أكدت عليه القواعد العامة في قانون العقوبات الأردني, وإن هذا الاقتناع قد يكون عند التحقيق (المدعي العام) لأنه يملك حرية التصرف في الدعوى وتحديد مصيرها وفق تقديره، غير أن مهمة هذا الأخير لا تعدو أن تكون مقصورة فقط على تقدير مدى كفاية الأدلة أو عدم كفايتها للاتهام وهي بذلك تختلف عن وظيفة قضاة الحكم الذين عليهم تقدير الأدلة القائمة من حيث كفايتها أو عدم كفايتها للحكم بالإدانة وبالتالي الاقتناع عند الحكم هي الأساس والجوهر.

ثانياً: النتائج المترتبة على مبدأ حرية اقتناع القاضي:

القناعة الشخصية للقاضي هي حجر الأساس في صدور الأحكام الجزائية وهذا ما ينطبق على الدليل الإلكتروني بكل خصائصه يجب أن لا يغير شيئاً من هذا المبدأ وهو ما يستشف من قانون العقوبات والقوانين الخاصة في الأردن من هذه الحرية.

والدليل الإلكتروني شأنه شأن الأدلة الجزائية بشكل عام لا يحظ أمام القاضي الجزائي بقوة حاسمة في الإثبات, وإنما هو مجرد دليل لا تختلف قيمته ولا تزيد حجته على سواه, وهذا أثر من آثار حرية القاضي الجزائي في الاقتناع بهذا الدليل أو عدم الاقتناع به لأنه قد لا ينطبق الدليل الإلكتروني مع ظروف الواقعة ملابساتها[42].

الفرع الثاني: ضوابط اقتناع القاضي بالدليل الإلكتروني:

تقدير قيمة الدليل في الإثبات بما فيه الدليل الإلكتروني يعود إلى قناعة قاضي الموضوع, وحرية التقدير هذه هي إحدى خصائص نظرية الإثبات الجزائي, ولكن إذا ما تعمقنا في دراسة هذه السلطة لا نجدها بأنها مطلقة وتحكمية وأنها من إطلاقاته, بل وضع المشرع لهذه السلطة ضوابط لم يتركها مطلقة, وهذه الضوابط هي بمنزلة صمام أمان إزاء انحراف القاضي عند ممارسته لها, كي لا تختل الأحكام ولا يصار إلى التحكم, إذ إن القاضي عليه تسبيب الأحكام تحت طائلة النقض, وأهم ما يتعلق بالإثبات الجزائي هو قناعة القاضي بالدليل الإلكتروني وأن المشرع الأردني وضع ضوابط لقناعة القاضي وهي بمثابة حماية وتطبيقاً للعدالة حتى لا تختل الأحكام ولا يصار إلى التحكم ولهذا يجب على القاضي تسبيب الأحكام في أي قرار يصدره وذكر السند القانوني.

وهناك نوعان من الضوابط :

أولاً: الضوابط المتعلقة بمحل الاقتناع:

اقتناع القاضي الجزائي بالأدلة الإلكترونية يكون من خلال أن يكون اساس الدليل الإلكتروني مشروع وأن يكون الاقتناع مبني على أدلة تم نظرها في الجلسة وناقشها الخصوم، بأن استوفت معيار العدالة العام بين جميع الأطراف.

1- مشروعية الدليل الإلكتروني:

إذا كان القانون يترك للقاضي الجزائي الحرية في أن يستمد اقتناعه من أي دليل وبأية وسيلة يراها موصلة إلى الحقيقة إلا أن هذه الحرية لا تعني أن القاضي الجزائي يستطيع أن يبني عقيدته على أي دليل يظفر به مهما مصدره ووسيلة البحث عنها, بل هو ملزم بضرورة أن يكون الدليل الذي يستند إليه في حكمه مقبولاً في الدعوى ولن يكون كذلك إلا بعد تيقنه من مراعاة الدليل لقاعدة المشروعية باتفاقه مع النظام القانوني في جملته, ويستعد في مقابل ذلك من المرافعة سائر الأدلة غير المقبولة, لأنها لا يمكن أن تدخل عنصراً عن عناصر تقديره, بل مخالفة هذا الشرط قد يهدر قيمة الدليل وتصف في النهاية قضائه بالبطلان, ولهذا فمشروعية الدليل الإلكتروني هي أساسية وأن محكمة التمييز الأردنية تؤكد على مبدأ المشروعية بقولها: أن الأدلة إقناعية والمحكمة ليست مقيدة في تكوين قناعتها بنوع معين من الأدلة شريطة أن تكون هذه الأدلة مقبولة قانوناً، وبالتالي أن حرية القاضي في طلب أي دليل أو استخلاصه يجب أن يكون هذا الدليل من حيث مصدره وطريقة البحث عنه مشروعة، وأن يكون هذا الدليل يتفق مع النظام القانوني وأن الأدلة غير المشروعة التي تخالف القانون يجب استبعادها من تقدير القاضي للقضية من أجل الفصل فيها سواء بالإدانة أو البراءة، وأن استعانت القاضي بدليل الإلكتروني مثلاً كان غير مشروع واستند القاضي في حكمه على هذا الدليل يؤدي إلى بطلان قرار القاضي لأن ما بني على باطل فهو باطل[43].

وبناءً على ما سبق فالخصومة الجزائية تقوم على التوازن بين ضمان حرية المتهم وسلطة الدولة في العقاب ولهذا يجب على القاضي أن لا يمارس سلطة العقاب على المتهم إلا إذا كان هناك دليل مشروع من جميع جوانبه، بأن تم مراعاة الضمانات التي نص عليها القانون والدستور والأردني، وبالتالي لا يجوز للقاضي أن يعتمد على دليل يستمد منه اقتناعه ويكون هذا الدليل باطلاً ومجرداً من القيمة القانونية في الاقتناع, بل لا بد أن يكون هذا الدليل مطابقاً للنصوص المقررة لضمانات الحرية الفردية وكذلك القواعد العامة للإجراءات الجزائية والمبادئ القانونية العامة كالقواعد والمبادئ التي توجب احترام قيم العدالة وأخلاقيتها والنزاهة في

الحصول على الأدلة واحترام حقوق الدفاع[44].

وكذلك فأن الدليل الإلكتروني يجب أن يكون مشروع وغير مخالف للقواعد القانونية والمبادئ القانونية، وقد أكدت على ما سبق التوصية رقم (18) للمؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات بقولها:- كل الأدلة التي تم الحصول عليها عن طريق انتهاك حق أساسي للمتهم والأدلة الناتجة عنها تكون باطلة ولا يمكن التمسُك بها أو مراعاتها في أي مرحلة من مراحل الإجراءات وقد أشار هذا المؤتمر إلى ضرورة احترام مبدأ المشروعية عند البحث عن الدليل في جرائم الحاسب الالي والجرائم التقليدية في بيئة تكنولوجيا المعلومات وإلا ترتب عليه بطلان الإجراء فضلاً في تقرير المسؤولية الجنائية لرجل السلطة العامة الذي انتهك القانون[45].

2- وضعية الدليل الإلكتروني:

من القواعد الأساسية في الإجراءات الجزائية, أنه يجب أن لا يبني القاضي حكمه على دليل لم تتم مناقشته في الجلسة، وهو ما يعبر عنه بوضعية الدليل, ولهذا يجب أن يكون للدليل أوراق وبينات ثابتة في الدعوى وأن يتاح إلى جميع الأطراف الاطلاع عليها ومناقشتها وأي دليل لا ينطبق عليه ما سبق يكون منعدم من ناحية قانونية لأنه يجب أن تدون جميع مراحل القضية منذ بداية حتى النهاية حتى يبني القاضي حكمه عليها, وغاية ذلك أن يكون الخصوم على بينة مما يقدم ضدهم من بينات حتى تتاح لهم أمكانية مناقشتهم والرد عليها, ولو لم يناقشوها بالفعل, إذ ليس من الضروري أن تحصل مناقشة علنية, كل ما يلزم هو أن تكون الأدلة في متناول الخصوم فحسب, وقد أكدت القواعد العامة والواقع العملي في المحاكم في الأردن على ما سبق

وعلة هذه القاعدة هي مبدأ الشفوية[46] في القضايا الجزائية هو مبدأ جوهري وأساسي تدعو له قواعد ومبادئ العدالة، ويجب على القاضي أن لا يكتفي بالأدلة سواء كانت تقليدية أم مستخرجه من الوسائل الإلكترونية, وإن سماع الشهود واعتراف المتهم نفسه بالإضافة إلى الاستماع إلى الخبراء ومن خلال مناقشة القاضي كل ما سبق يساعد بشكل واضح وكبير على تكوين قناعة القاضي والحكم في القضية سواء بالبراءة أو الإدانة، وأن مبدأ شفوية يساعد الأطراف كذلك في مواجهة كل خصم خصمه بما لديه من أدلة واقتناعهم بأنهم قدموا وعملوا ما يقدرون عليه وهذا يساعد على استقرار مبدأ العدالة في نفوسهم، وبالتالي مبدأ الشفوية هو ضابط يراقب قناعة القاضي.

والدليل الإلكتروني يعتبر من أدلة الإثبات سواء كان على شكل بيانات معروضة على شاشة الكمبيوتر أو أقراص ممغنطة أو معلومات مستخرجة من الأجهزة الإلكترونية كل هذه الأدلة وغيرها ستكون محل نقاش عند القاضي، وبناءً على ما سبق يمكن القول أنه لا يجوز أن يقضي القاضي بناء على معلوماته الشخصية وكذلك يجب أن يتم عمل دورات وندوات للقضاة فيما يتعلق بالأدلة الإلكترونية؛ لأن الأجهزة الإلكترونية في تطور مستمر ويجب أن يواكب هذا التطور فهم وإدراك لتطور هذه الأدلة الإلكترونية حتى يتمكن القاضي من الفصل في هذه القضايا ومنها جريمة الإرهاب الإلكتروني لأن قرار القاضي هو يتعلق ويرتبط بمصير إنسان سواء بالبراءة أو الإدانة ويجب على القاضي أن يقرر هو ليس الخبير الذي يستعين فيه لأن القاضي يعتبر هو الخبير الأعلى.

ثانياً: ضوابط متعلقة بدرجة الاقتناع وسماته:

القاضي الجزائي هو حر في تقدير الأدلة وموازنتها ولكنه مقيد بتأسيس اقتناعه على الجزم واليقين, دون الظن والترجيح والاحتمال من ناحية, وأن يكون متوائماً مع مقتضيات العقل والمنطق من ناحية أخرى, وأن المتهم وفق الأدلة الإلكترونية التي تم عرضها عليه وتم مناقشتها يصدر بأنه القرار أما بريء أو مدان.

1- وصول الاقتناع القضائي حد الجزم واليقين:

القاضي يجب أن يصل إلى الجزم واليقين وأن اليقين هو كل معرفة لا تقبل الشك ومنها الأدلة العلمية التي لا تقبل الشك وتعرض نفسها على العقل، وقد يسمى التسليم بأمر ظاهر أو راجح يقيناً اقتناعاً أو شبه يقين.

العلم اليقيني:- وهو الذي ينكشف فيه المعلوم انكشافاً لا يبقى معه ريب ولا يقاربه إمكان الغلط أو الوهم[47].

اليقين كمصطلح قانوني:- عبارة عن اقتناع مستند إلى حجج ثابتة وقطعية[48] أو حالة ذهنية أو عقلانية تؤكد وجود الحقيقة[49].

والقاضي الجزائي عندما يصل إلى درجة اليقين فإنه يقوم بإصدار حكمه بالبراءة أو الإدانة والأصل في الإنسان هو البراءة وهذا ما أكده قانون العقوبات الأردني ونتيجة لذلك يجب على القاضي عند إصدار حكمه أن يبنيه على اليقين والجزم لا شك والاحتمال وهذا اليقين يجب أن يكون في جميع الأدلة ومنها الدليل الإلكتروني, ومتى ما تكامل اليقين بأن وصل القاضي إلى

درجة القطع ينشأ ما يسمى بالاقتناع اليقيني، وهو أساس الحقيقة القضائية التي ينشدها القاضي في حكمه.

والقاضي الجزائي قد يصل إلى درجة اليقين من خلال الأدلة الإلكترونية التي تعرض عليه ويقدر مدى قوتها وضعفها في نسبتها إلى المتهم في هذه الجريمة، وأن اقتناع القاضي من خلال نوعين من المعرفة وهي المعرفة الحسيّة التي تدركها الحواس والمعرفة العقلية التي يقوم بها القاضي عن طريق التحليل والاستنتاج من خلال الربط بين هذه المخرجات والملابسات التي أحاطت بها إلا أنه في نطاق الجزم بوقوع جريمة الإرهاب الإلكتروني ونسبتها إلى المتهم تتطلب نوعاً جديداً من المعرفة العلمية للقاضي بالأدلة الإلكترونية وبتكنولوجيا المعلومات بشكلٍ عام حتى يتم إزالة أي شك أو غموض لدى القاضي، وأن أي شك لدى القاضي يجب أن يتم تفسيره لمصلحة المتهم.

2- كون الاقتناع القضائي متوائماً مع مقتضيات العقل والمنطق:

الاقتناع القضائي يجب أن ينبني عملية منطقية تقوم الاستقراء والاستنباط ينتهي في ختامها إلى نتيجة معينة, فالقاضي وإن كان حراً في أن يعتقد في قيمة الأدلة سواء التقليدية أم الإلكترونية المطروحة ولكنه لا يملك التحكم في هذا الاعتقاد، فاليقين المطلوب من القاضي وهو الذي يصل إليه القاضي بناء على العقل والمنطق[50] وبالتالي يجب أن تكون الأدلة الإلكترونية التي اعتمد عليها القاضي في حكمه تتفق مع العقل والمنطق.

الخاتمة

الإرهاب الإلكتروني هو الخطر الجديد الذي يهدد العالم بأسره في عصر المعلوماتية حيث أن العالم يدفع ضريبة التطور التقني بخطر جديد لم يكن متصوراً من قبل وهذا الخطر مرتبط بالتطور التقني ويزداد خطورة وتعقيداً بازدياد التطور التقني الأمر الذي يستوجب وقفة جدية لمحاربة هذا الخطر وهذا يكون من خلال الإثبات الجنائي في جرائم الإرهاب الإلكتروني.

وأن جرائم الإرهاب الإلكتروني تقوم على مبدأ حرية الإثبات ولهذا يجوز تقديم أي دليل سواء دليل إدانة من قبل النيابة العامة أو دليل براءة من قبل المتهم وعلى الرغم من الاعتقاد السائد أن النيابة العامة تقدم فقط أدلة إدانة ضد المتهم ولكن في الواقع العملي قد تقدم أدلة تؤدي إلى براءة متهم، وأن القاضي الجزائي نظراً لطبيعة الخاصة لهذه الأدلة قد يستعين بخبراء ورغم ذلك فإن القاضي هو الخبير الأعلى الذي يقدر هذه الخبرة الإلكترونية والأدلة الإلكترونية.

وفي نهاية البحث قد توصل الباحث إلى مجموعة من النتائج والتوصيات يمكن إدراجها على النحو الآتي:

النتائج:

1) القواعد العامة الجزائية تفترض بأن الإثبات الجزائي يكون بكافة طرق الإثبات وهذا ما ينطبق كذلك على جريمة الإرهاب الإلكتروني وفقاً لقانون الجرائم الإلكترونية الأردني رقم (27) لسنة 2015م, وكذلك فأن من أهم مميزات جريمة الإرهاب الإلكتروني عن غيرها من الجرائم هو أنها تحتاج إلى وسائل إثبات حديثة تكون بنفس مواصفات وتميز طريقة ارتكاب هذه الجريمة ولهذا فإن الوسائل المساعدة في الإثبات هي داعم ومساند لرجال الضابطة العدلية في تقديم الأدلة وللمحكمة المختصة في إدانة أو براءة المتهم في جريمة الإرهاب الإلكتروني.

2) النيابة العامة في الأردن ويساعدها رجال الضابطة العدلية هي من تقوم بإجراء التفتيش في الجرائم الإلكترونية وخاصة جريمة الإرهاب الإلكتروني بعد الحصول على أذن المدعي العام المختص, وللنيابة العامة سلطة واسعة في التفتيش وفق القواعد العامة وبالتالي يجوز تفتيش مكونات الحاسوب المادية والمعنوية وشبكات الحاسوب وأن يمتد التفتيش لجهاز حاسوب موجود في مكان آخر مرتبط بنهاية طرفيه متصلة بجهاز حاسوب المتهم و قد حسم الخلاف الفقهي وأجاز ضبط ومصادرة المكونات المادية والمعنوية للحاسب الآلي وكل ذلك تحت رقابة من المحكمة المختصة بذلك, وهذه الضابطة العدلية هي التي تقيم الدليل على المتهم بالإدانة ولكن يتدخل القاضي الجزائي لأن دوره ليس دور سلبي كالقاضي المدني (يقتصر على الموازنة بين الأدلة التي يقدمها الأطراف ويرجح إحداهما) ولهذا فالقاضي الجزائي يكون له دور إيجابي يبحث عن الأدلة بهدف الوصول إلى الحقيقة, بأن يصل إلى مرحلة الجزم واليقين لإصدار قرار بالبراءة أو الإدانة عن طريق اتخاذ أي إجراء يراه مناسباً والقاضي الجزائي له حرية الاقتناع وكل ذلك حتى يقوم بالفصل في القضية وفق القانون والعدالة.

3) المشرع الأردني اعتبر جريمة الإرهاب الإلكتروني هي جريمة شكلية تتحقق بمجرد الدخول غير المشروع أو إنشاء موقع إرهابي أو نشر معلومات إرهابية, أي أن المشرع يفترض أن هناك جريمة إرهاب إلكتروني قائمة إذا تحقق معها الركن المعنوي دون أن تلزم النيابة العامة بإثبات علاقة السببية بين الفعل والنتيجة.

التوصيات:

1) أتمنى على المشرع الأردني تأهيل قضاة متخصصين فقط في نظر جرائم الإرهاب الإلكتروني، فالتخصص الدقيق في قضايا مهمة وخطيرة على الدولة الأردنية يساعد على زيادة إدراك وفهم القاضي لهذه الجريمة وما هي المداخل القانونية التي قد يستغلها المتهم في ارتكاب جريمة الإرهاب الإلكتروني وبالتالي من قضية إلى قضية أخرى يصبح القاضي أكثر خبرة من الخبراء أنفسهم وهذا مطلوب لأن القاضي هو الخبير الأعلى.

2) أتمنى على خبراء الإنترنت من الأجهزة الحكومية ومطوري التكنولوجيا في الأردن بتطوير وسائل الإثبات في جريمة الإرهاب الإلكتروني ضد من يقوم بهذه الجريمة حتى لا يصبح هذا الفضاء الإلكتروني ساحة حرب دامية موجهة ضد دول العالم وخاصة في الأردن لأن الإرهاب لا دين له والإرهاب لا يعرف حدود وكذلك أتمنى على المشرع الأردني تغليظ العقوبات على مرتكبي جرائم الإرهاب الإلكتروني لأن الردع العام واجب في مثل هذه الجرائم, وأتمنى تدريس مادة في كليات الحقوق في الأردن عن الإرهاب الإلكتروني بكل جوانبه وتكون هذه المادة إجبارية وليست اختيارية

3) أتمنى على الإعلام الأردني مزيد من الدقة والأمانة في المعلومات التي يقومون بنشرها وخاصة فيما يتعلق بالإرهاب لأن الواقع العملي أثبت أن الإعلام يعتبر هو السلطة الرابعة في الدولة بل هو السلطة الأولى للدولة لأنه قد يحرك الشعب أو يهدئه.

الهوامش

(1) إبراهيم (2010)، فن التحقيق الجنائي في الجرائم الإلكترونية ,ط1 ,دار الفكر الجامعي ,الإسكندرية –مصر.

(2) كامل، السعيد (2005)، شرح قانون أصول المحاكمات الجزائية، دار الثقافة، عمان– الأردن.

(3) (قانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015,المادة 13/أ)

(4) الطوالبة، علي (2003)، التفتيش الجنائي على نظام الحاسوب، أطروحة دكتوراه، جامعة عمان العربية للدراسات العليا، عمان– الأردن.

(5)عاكوم، القاضي وليد (2003)، التحقيق في جرائم الحاسوب، مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي– الإمارات.

(6) الربيش، عبد الله بن صالح بن الرشيد (1434ه)، رسالة القاضي الجنائي في تقدير أدلة الإثبات بين الشريعة والقانون وتطبيقاتها في المحاكمة العربية السعودية، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض– السعودية.

(7)محمود، عبد الله حسين (2003)، إجراءات جمع الأدلة في مجال المعلوماتية، مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي– الإمارات.

(8) عفيفي، عفيفي كامل (2000)، جرائم الكمبيوتر، دون ناشر، القاهرة– مصر.

(9)خليل، عزه محمود (1994)، مشكلات المسؤولية المدنية في مواجهة فيروس الحاسوب، أطروحة الدكتوراه، جامعة القاهرة، القاهرة– مصر.

(10) رستم، هشام (1992)، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط– مصر.

(11) البربري، صالح (2003)، دور الشرطة في مكافحة جرائم الإنترنت، مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي– الإمارات.

(12)عياد، محمد علي سالم (1996)، الوسيط في شرح قانون أصول المحاكمات الجزائية، ج2، دار الثقافة، عمان– الأردن.

(13) (قانون أصول المحاكمات الجزائية الأردني, المادة 87)

(14)عقيدة، محمد أبو العلا (2003)، التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي– الإمارات.

(15) (قانون الجرائم الإلكترونية الأردني, المادة 13/ب)

(16) (قانون الجرائم الإلكترونية الأردني, المادة 13/ج)

(17)عبد الحميد، محمد فاروق (1999)، القواعد الفنية الشرطية للتحقيق والبحث الجنائي، رسالة ماجستير، أكاديمية نايف العربية للعلوم الأمنية، الرياض– السعودية.

(18)عبد الحميد، محمد فاروق (1999)، القواعد الفنية الشرطية للتحقيق والبحث الجنائي، رسالة ماجستير، أكاديمية نايف العربية للعلوم الأمنية، الرياض– السعودية.

(19)بحر، عبد الرحمن (1999)، معوقات التحقيق في جرائم الإنترنت، رسالة ماجستير، أكاديمية نايف العربية للعلوم الأمنية، الرياض– السعودية.

(20)عبد الحميد، محمد فاروق (1999)، القواعد الفنية الشرطية للتحقيق والبحث الجنائي، رسالة ماجستير، أكاديمية نايف العربية للعلوم الأمنية، الرياض– السعودية.

(21) العنزي، سليمان (2003)، وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير، أكاديمية نايف العربية للعلوم الأمنية،

الرياض- السعودية.
(22) عبد الحميد، محمد فاروق (1999)، القواعد الفنية الشرطية للتحقيق والبحث الجنائي، رسالة ماجستير، أكاديمية نايف العربية للعلوم الأمنية، الرياض- السعودية.
(23) البشري، محمد الأمين (2004)، التحقيق في جرائم الحاسب الآلي والإنترنت، الطبعة الأولى، جامعة نايف العربية للعلوم الأمنية، الرياض- السعودية.
(24)الفتوح، عبد القادر (دون سنة)، المسرح الإلكتروني، موقع جريدة الرياض على الإنترنت: www.alriydh.com.sa/kpage.asp3art.37753
(25)البشري، محمد الأمين (2004)، التحقيق في جرائم الحاسب الآلي والإنترنت، الطبعة الأولى، جامعة نايف العربية للعلوم الأمنية، الرياض- السعودية.
(26) العنزي، سليمان (2003)، وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير، أكاديمية نايف العربية للعلوم الأمنية، الرياض- السعودية.
(27) داود، حسن (2000)، جرائم نظم المعلومات، رسالة ماجستير، أكاديمية نايف العربية للعلوم الأمنية، الرياض- السعودية.
(28) (موقع على الإنترنت: www.arabiat.com)
(29) الغافري، حسين (دون سنة)، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الحاسوب، بحث منشور على موقع قوانين الشرق على شبكة الإنترنت: www.eastlaw.com
(30)عبد المطلب، ممدوح عبد الحميد (2001)، جرائم استخدام الحاسب الالي وشبكة المعلومات العالمية، مكتبة دار الحقوق الشارقة- الإمارات.
(31)الغافري، حسين (دون سنة)، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الحاسوب، بحث منشور على موقع قوانين الشرق على شبكة الإنترنت: www.eastlaw.com
(32)العنزي، سليمان (2003)، وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير، أكاديمية نايف العربية للعلوم الأمنية، الرياض- السعودية.
(33)محمد، فاضل زيدان (2006)، سلطة القاضي الجنائي في تقدير الأدلة "دراسة مقارنة"، دار الثقافة، عمان- الأردن.
(34)خليل، أحمد ضياء الدين محمد (1982)، مشروعية الدليل في المواد الجنائية- دراسة تحليلية مقارنة لنظريتي الإثبات والمشروعية في مجال الإجراءات الجزائية، أطروحة دكتوراه، جامعة عين شمس، القاهرة- مصر.
(35) (قرار محكمة التمييز الأردنية رقم 2006/542 ,نظام عدالة)
(36) حسني، محمود نجيب (1988)، شرح قانون الإجراءات الجنائية، الطبعة الثانية، دار النهضة العربية، القاهرة، مصر.
(37) الرشيد، غازي عبد الرحمن هيان (2004)، الحماية القانونية من جرائم المعلوماتية (الحاسب والإنترنت)، أطروحة دكتوراه، جامعة بيروت، لبنان.
(38) أحمد، هلالي عبد الله (2008)، حجية المخرجات الكمبيوترية في المواد الجنائية، الطبعة الثانية، دار النهضة العربية، القاهرة- مصر.
(39) حسني، محمود نجيب (1988)، شرح قانون الإجراءات الجنائية، الطبعة الثانية، دار النهضة العربية، القاهرة، مصر.
(40)الربيش، عبد الله بن صالح بن الرشيد (1434هـ)، رسالة القاضي الجنائي في تقدير أدلة الإثبات بين الشريعة والقانون وتطبيقاتها في المحاكمة العربية السعودية، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض- السعودية.
(41) الطوالبة، علي (2003)، التفتيش الجنائي على نظام الحاسوب، أطروحة دكتوراه، جامعة عمان العربية للدراسات العليا، عمان- الأردن.
(42) الصغير، جميل عبد الباقي (2002)، أدلة الإثبات الجنائي التكنولوجيا الحديثة- دراسة مقارنة، دار النهضة العربية، القاهرة- مصر.
(43) (محكمة التمييز الأردنية في قرارها رقم 119 السنة 1954)
(44) الربيش، عبد الله بن صالح بن الرشيد (1434هـ)، رسالة القاضي الجنائي في تقدير أدلة الإثبات بين الشريعة والقانون وتطبيقاتها في المحاكمة العربية السعودية، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض- السعودية.
(45) الرشيد، غازي عبد الرحمن هيان (2004)، الحماية القانونية من جرائم المعلوماتية (الحاسب والإنترنت)، أطروحة دكتوراه، جامعة بيروت، لبنان.
(46) عبيد، رؤوف (دون سنة)، المشكلات العملية في الإجراءات الجنائية، الجزء الأول، الطبعة الثانية، دار الفكر العربي، القاهرة- مصر.
(47)مدكور، إبراهيم (1983)، المعجم الفلسفي، دار الكتاب، القاهرة- مصر.
(48) عبد الله، موسى مسعود رحومة (1988)، حرية القاضي الجنائي في تكوين عقيدته "دراسة مقارنة"، الدار الجماهيرية للنشر والتوزيع، الجزائر.
(49)أحمد، هلالي عبد الله (2008)، حجية المخرجات الكمبيوترية في المواد الجنائية، الطبعة الثانية، دار النهضة العربية، القاهرة- مصر.
(50) الربيش، عبد الله بن صالح بن الرشيد (1434هـ)، رسالة القاضي الجنائي في تقدير أدلة الإثبات بين الشريعة والقانون وتطبيقاتها في المحاكمة العربية السعودية، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض- السعودية.

المصادر والمراجع

أولاً: الكتب:

البشري، محمد الأمين (2004)، التحقيق في جرائم الحاسب الآلي والإنترنت، الطبعة الأولى، جامعة نايف العربية للعلوم الأمنية، الرياض- السعودية.

إبراهيم، خالد ممدوح (2009)، الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية- مصر.

عياد، سامي حامد (2008)، استخدام تكنولوجيا المعلومات في مكافحة الإرهاب، دار الفكر الجامعي، ط1، الاسكندرية- مصر.

الصغير، جميل عبد الباقي (1992)، القانون الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة- مصر.

الطوالبة، علي حسن (2009)، مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي دراسة مقارنة، مركز الإعلام الأمني، عمان- الأردن.

كامل، السعيد (2005)، شرح قانون أصول المحاكمات الجزائية، دار الثقافة، عمان- الأردن.

رستم، هشام (1992)، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط- مصر.

عفيفي، عفيفي كامل (2000)، جرائم الكمبيوتر، دون ناشر، القاهرة- مصر.

عياد، محمد علي سالم (1996)، الوسيط في شرح قانون أصول المحاكمات الجزائية، ج2، دار الثقافة، عمان- الأردن.

عبد المطلب، ممدوح عبد الحميد (2001)، جرائم استخدام الحاسب الالي وشبكة المعلومات العالمية، مكتبة دار الحقوق الشارقة- الإمارات.

محمد، فاضل زيدان (2006)، سلطة القاضي الجنائي في تقدير الأدلة "دراسة مقارنة"، دار الثقافة، عمان- الأردن.

عبد الله، موسى مسعود رحومة (1988)، حرية القاضي الجنائي في تكوين عقيدته "دراسة مقارنة"، الدار الجماهيرية للنشر والتوزيع، الجزائر.

حسني، محمود نجيب (1988)، شرح قانون الإجراءات الجنائية، الطبعة الثانية، دار النهضة العربية، القاهرة، مصر.

أحمد، هلالي عبد الله (2008)، حجية المخرجات الكمبيوترية في المواد الجنائية، الطبعة الثانية، دار النهضة العربية، القاهرة- مصر.

الصغير، جميل عبد الباقي (2002)، أدلة الإثبات الجنائي التكنولوجيا الحديثة- دراسة مقارنة، دار النهضة العربية، القاهرة- مصر.

عبيد، رؤوف (دون سنة)، المشكلات العملية في الإجراءات الجنائية، الجزء الأول، الطبعة الثانية، دار الفكر العربي، القاهرة- مصر.

مدكور، إبراهيم (1983)، المعجم الفلسفي، دار الكتاب، القاهرة- مصر.

25)إبراهيم ,خالد ممدوح (2008),أمن الجريمة الإلكترونية ,الدار الجامعية ,الإسكندرية – مصر.

26) إبراهيم ,خالد ممدوح (2010),فن التحقيق الجنائي في الجرائم الإلكترونية ,ط1 ,دار الفكر الجامعي ,الإسكندرية –مصر.

ثانياً:- رسائل الماجستير والدكتوراه:-

الطوالبة، علي (2003)، التفتيش الجنائي على نظام الحاسوب، أطروحة دكتوراه، جامعة عمان العربية للدراسات العليا، عمان- الأردن.

محمود، عبدالله حسين (2001)، سرقة المعلومات المخزنة بالحاسوب، أطروحة دكتوراه، جامعة عين شمس، القاهرة- مصر.

خليل، عزه محمود (1994)، مشكلات المسؤولية المدنية في مواجهة فيروس الحاسوب، أطروحة الدكتوراه، جامعة القاهرة، القاهرة- مصر.

عبد الحميد، محمد فاروق (1999)، القواعد الفنية الشرطية للتحقيق والبحث الجنائي، رسالة ماجستير، أكاديمية نايف العربية للعلوم الأمنية، الرياض- السعودية.

العنزي، سليمان (2003)، وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير، أكاديمية نايف العربية للعلوم الأمنية، الرياض- السعودية.

داود، حسن (2000)، جرائم نظم المعلومات، رسالة ماجستير، أكاديمية نايف العربية للعلوم الأمنية، الرياض- السعودية.

بحر، عبد الرحمن (1999)، معوقات التحقيق في جرائم الإنترنت، رسالة ماجستير، أكاديمية نايف العربية للعلوم الأمنية، الرياض- السعودية.

خليل، أحمد ضياء الدين محمد (1982)، مشروعية الدليل في المواد الجنائية- دراسة تحليلية مقارنة لنظريتي الإثبات والمشروعية في مجال الإجراءات الجزائية، أطروحة دكتوراه، جامعة عين شمس، القاهرة- مصر.

الرشيد، غازي عبد الرحمن هيان (2004)، الحماية القانونية من جرائم المعلوماتية (الحاسب والإنترنت)، أطروحة دكتوراه، جامعة بيروت، لبنان.

الربيش، عبد الله بن صالح بن الرشيد (1434هـ)، رسالة القاضي الجنائي في تقدير أدلة الإثبات بين الشريعة والقانون وتطبيقاتها في المحاكمة العربية السعودية، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض- السعودية.

ثالثاً: المؤتمرات:

عطية، أيسر محمد (2014)، دور الآليات الحديثة للحد من الجرائم المستحدثة الإرهاب الإلكتروني وطرق مواجهته،الملتقى العلمي الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية،كلية العلوم الإستراتيجية،الأردن.

البربري، صالح (2003)، دور الشرطة في مكافحة جرائم الإنترنت، مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي– الإمارات.

عاكوم، القاضي وليد (2003)، التحقيق في جرائم الحاسوب، مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي– الإمارات.

محمود، عبد الله حسين (2003)، إجراءات جمع الأدلة في مجال المعلوماتية، مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي– الإمارات.

عقيدة، محمد أبو العلا (2003)، التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي– الإمارات.

حمودة، علي محمود علي (2003)، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، بحث مقدم ضمن أعمال المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية ونظمته أكاديمية شرطة دبي، دبي– الإمارات.

رابعاً:– الأبحاث:–

إبراهيم، خالد ممدوح (دون سنة)، الدليل الإلكتروني في جرائم المعلوماتية، بحث منشور على الموقع الآتي:– http//kenamaonline.com/asers/khaledMamdoah/posts/793H5

الغافري، حسين (دون سنة)، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الحاسوب، بحث منشور على موقع قوانين الشرق على شبكة الإنترنت: www.eastlaw.com

البشري، محمد (2004)، التحقيق في جرائم الحاسب والإنترنت، المجلة العربية للدراسات الأمنية والتوريد، عدد 33، القاهرة– مصر.

الفتوح، عبد القادر (دون سنة)، المسرح الإلكتروني، موقع جريدة الرياض على الإنترنت: www.alriydh.com.sa/kpage.asp3art.37753

خامساً :قرارات المحاكم :

قرار محكمة التمييز الأردنية بصفتها الجزائية رقم 2009/752 ,منشورات نظام عدالة .

قرار محكمة التمييز الأردنية رقم 2006/542 ,نظام عدالة.

قرار محكمة التمييز الأردنية بصفتها الجزائية رقم 1994/338 , منشورات نظام عدالة .

قرار محكمة التمييز الأردنية بصفتها الجزائية رقم 1993/169 ,المنشور على الصفحة 2489 من عدد مجلة نقابة المحامين بتاريخ 1993/1/1 .

قرار محكمة التمييز الأردنية بصفتها الجزائية رقم 1956/33 ,المنشور على الصفحة 217 من عدد مجلة نقابة المحامين بتاريخ 1956/1/1.

Criminal Evidence In The Crimes Of Electronic Terrorism In Accordance With Jordanian Law

Malek Nadi Salem *

Abstract

Criminal evidence is the establishment of evidence before the judiciary in the ways determined by the law on the existence of a legal fact that has caused its effects, and the crime so that it can be attributed to the perpetrator ,there must be an evidence to prove that he is involved; because the theory of evidence based on the fact that the right bare from the evidence does not exist, And is no longer at the time of conflict and that the criminal evidence is to establish evidence of the occurrence of the crime and attributed to a certain actor, This guide provides a scientific and legal method that can be used to prove crime through electronic information systems. It also helps to develop the academic understanding of the electronic guide provided to law enforcement and support agencies. Authenticity of electronic outputs in penal matters. This electronic terrorism is through the use of digital techniques to intimidate and subjugate others. This is often politically, ethnically or religiously motivated. It is considered one of the most dangerous types of terrorism in the present era due to the widespread use of modern technology in the world. evidence that may be obtained in a legitimate manner in accordance with the principle of legality and electronic evidence. There is no physical evidence or other traditional evidence present in the electronic crime. The judiciary resorts to the assignment of experts to conduct the disclosure and verification of the contents of the electronic documents and then to present the report, which is the evidence and not the electronic documents, but a method of intimidation of some legal systems rather than opposing the bases and purposes of conducting the experiment and its nature. As evidence for discussion, objection, rejection and acceptance.

Keywords: Electronic terrorism; criminal evidence, information systems.

---

* Faculty of Law, The University of Jordan. Received on 17/1/2018 and Accepted for Publication on 16/9/2018.